What is claimed is:

1. A method of achieving context-sensitive confidentiality among security domains within a federated environment, the method comprising steps of:

determining a route to be taken by a message to be transmitted in the federated environment, where the route spans a plurality of the security domains;

determining rights of nodes to be encountered on the determined route to access security-sensitive portions of the message;

selectively protecting the security-sensitive portions of the message, according to the determined access rights; and

transmitting the message with its selectively-protected portions on the determined route.

2. The method according to Claim 1, wherein the selectively protecting step further comprises the step of encrypting at least one security-sensitive portion of the message.

3. The method according to Claim 1, wherein the selectively protecting step further comprises the step of computing a digital signature over at least one security-sensitive portion of the message.

4. The method according to Claim 1, wherein the step of determining the route further comprises the step of consulting policy to determine the route to be taken for this message.

5. The method according to Claim 1, wherein the step of determining the access rights

further comprises the step of consulting policy for each of the nodes to be encountered.

6. The method according to Claim 1, further comprising the step of determining a role of at least one of the nodes to be encountered, and wherein the step of determining the access rights further comprises the step of consulting policy for each determined role, wherein the policy specifies access rights for that role.

7. The method according to Claim 1, wherein the selectively protecting step further comprises the step of encrypting each security-sensitive portion of the message for each node determined to have access rights to that portion.

8. The method according to Claim 7, wherein the encrypting step uses a public key associated with each of the nodes for which the encrypting step operates.

9. The method according to Claim 1, wherein the determined route is specified in the transmitted message.

10. The method according to Claim 1, further comprising the step of determining a role of at least one of the nodes to be encountered, and wherein the selectively protecting step further comprises the step of encrypting each security-sensitive portion of the message for each of the roles that are determined to have access rights to that portion.

11. The method according to Claim 10, wherein the encrypting step uses a public key associated with each of the roles for which the encrypting step operates.

12. The method according to Claim 1, further comprising the steps of:

receiving the transmitted message at a selected one of the nodes on the determined route; and

securely accessing only those ones of the selectively-protected portions of the received message to which the selected node has access rights.

13. The method according to Claim 1, wherein the transmitted message contains information identifying an authentication authority from a first of the security domains, and indicates that this authentication authority has already authenticated a party for which the message requests access to services, such that nodes receiving the message in other ones of the security domains can bypass authentication of the party for access to services of that other security domain, upon verifying authenticity of the authentication authority and establishing that the authentication authority vouches for the received message.

14. The method according to Claim 13, wherein the authentication authority is determined to vouch for the received message if a digital signature computed by the authentication authority and transmitted with the message is determined, by the node receiving the message in the one of the other security domains, to be valid.

15. The method according to Claim 13, wherein the transmitted message contains security credentials of the party, where those security credentials have been authenticated by the identified authentication authority and are protected such that only authorized ones of the nodes receiving the message in other ones of the security domains can access the protected security credentials.

16. The method according to Claim 15, wherein the protected security credentials are encrypted using a public key of each of the authorized ones of the nodes receiving the message, such that each of the authorized ones can decrypt the protected security credentials using a corresponding private key.

17. A system for achieving context-sensitive confidentiality among security domains within a federated environment, the system comprising:

means for determining a route to be taken by a message to be transmitted in the federated environment, where the route spans a plurality of the security domains;

means for determining rights of nodes to be encountered on the determined route to access security-sensitive portions of the message;

means for selectively protecting the security-sensitive portions of the message, according to the determined access rights; and

means for transmitting the message with its selectively-protected portions on the determined route.

18. A computer program product for securely transmitting context-sensitive confidential

message content among security domains within a federated environment, the computer program product embodied on one or more computer-readable media and comprising:

computer-readable program code means for determining a route to be taken by a message to be transmitted in the federated environment, where the route spans a plurality of the security domains;

computer-readable program code means for determining rights of nodes to be encountered on the determined route to access security-sensitive portions of the message;

computer-readable program code means for selectively protecting the security-sensitive portions of the message, according to the determined access rights; and

computer-readable program code means for transmitting the message with its selectively-protected portions on the determined route.

19. A method of providing a message confidentiality service for securely transmitting messages among security domains within a federated environment, the method comprising steps of:

determining a route to be taken by a message to be transmitted in the federated environment, where the route spans a plurality of the security domains;

determining rights of nodes to be encountered on the determined route to access security-sensitive portions of the message; and

determining how the security-sensitive portions of the message should be protected, according to the determined access rights.

20. The method according to Claim 20, further comprising the step of charging a fee for one or more of the determining steps.

21. The method according to Claim 20, further comprising the step of applying the determined protections to the security-sensitive portions.